UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/688,490	10/16/2000	Juan A. Garay	Garay 4-1-10 (8018-21)	3241

7590 01/30/2004

Joseph B. Ryan
Ryan Mason & Lewis, LLP
90 Forest Ave.
Locust Valley, NY 11560

EXAMINER	
MASHAAL, ALI M	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 01/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/688,490	Applicant(s) GARAY ET AL.	
	Examiner Ali M. Mashaal	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-23* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) □ The translation of the foreign language provisional application has been received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

4) □ Interview Summary (PTO-413) Paper No(s). _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other:

DETAILED ACTION

1. This action is in response to the application filed on 10/16/2000.

2. Claims 1-23 are under examination.

Specification

3. The disclosure is objected to because of the following informalities: On page 1, line 13,there appears to be a typo, where the sentence reads: "Keys are allocated in such a way hat users…" "hat" should be replaced with "that."

The specification should be reviewed, and all typos and errors must be corrected. Appropriate correction is required.

Claim Objections

4. Claim 10 is objected to because of the following informalities: The claim is not terminated with a (.) period. Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 7-10, 22, and 23 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by "Coding for Blacklisting Problems Without Computational Assumptions" to Kumar et al. (Kumar).

As per claims 7 and 22, Kumar teaches a broadcast encryption method, comprising the steps of: allocating a set of subscriber keys to each of a plurality of n subscribers, wherein each set... see page 616 "3 The Overall Construction" in which it is stated that "each user x gets assigned some subset Sx of u out of the m keys." As per broadcasting encrypted content to the n subscribers using a set of broadcast keys Sp selected from the universal set of keys, see page 616 "3 The Overall Construction" first paragraph. As per identifying at least one compromised subscriber key, see paragraph one which states that pieces corresponding to excluded users are discarded. Kumar's Exclusion of users constitutes identifying the claimed compromised subscriber key. As per adjusting Sp by excluding the at least one compromised subscriber key see page 616 "3 The Overall Construction", paragraph 2: "The pieces corresponding to keys belonging to users who have been excluded are then discarded.." As per "updating a set..." see page 616 "3 The Overall Construction" paragraph 2 "and the remaining encrypted pieces are broadcast to all users. By decrypting the pieces corresponding to the keys that each valid user has, the user reconstructs the original message". Also see page 617 "The Outer Code".

As per claims 8, and 23, Kumar teaches "Wherein the step of allocating is performed using a randomized…." See page 614 "2 Cover-Free Set Systems" and page 618-619 "4 A Randomized Construction".

As per claim 9, see page 611-612, "Our Approach".

As per claim 10, see page 616, "2.4 Warmup..".

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.1 Claims 1-4, 6, 7, 11-13, and 18, 19, 21, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Efficient Methods for Integrating Traceability and Broadcast Encryption" to Gafni et al. (Gafni) in view of "Key Management for Multicast: Issues and Architecture" to Wallner et al. (Wallner).

As per claims 1, 7, 18, and 22, Gafni teaches a broadcast encryption method comprising the steps of: "broadcasting…" (See p. 372 "Introduction", which is p. 1 of the document provided).

As per "modifying…" and "updating…", Gafni directs the reader to Wallner, but does not explicitly teach "modifying…" and "updating…" (see p. 377, 3rd complete paragraph).

However, Wallner in an analogous art, teaches "modifying..." and "updating..." (see p. 4, "5.1 Manual Key Distribution", as well as p. 6 &7 "5.4 Hierarchical Tree Approach")

It would have been obvious to one having ordinary skill in the art at the time the invention was made to use Wallner's method to resolve the issue of compromised keys. One would have been motivated to do so since Gafni suggested making this modification (see p. 377, 3rd complete paragraph).

As per claims 2 and 11, Gafni further discloses the use of smart cards having sets of subscriber keys encoded thereon (see page 382, lines 4-7).

As per claims 3, 12, and 19 although not explicitly disclosed in the Gafni disclosure, it would have been obvious to one having ordinary skill in the art at the time the invention was made to identify a compromised smartcard; and identify each subscriber key contained on the compromised smartcard as a compromised key, because doing so does not part from the spirit of Gafni's invention.

As per claims 4 and 13, Gafni suggests the base claim 3, and further teaches the compromised keys are those of an excluded subscriber (see pages 7 and 8, "5.4.1 The Exclusion Principle").

As per claims 6 and 21, the Gafni-Wallner combination teaches base-claim 1, but fails to teach "the first predetermined threshold is one key." However, Wallner further teaches a single Net keying having to be replaced by an alternative Net key in the event that the single Net key is compromised, (see p. 4, "5.1 Manual Key Distribution"). This constitutes the first predetermined threshold being 1. It would have been obvious to one having ordinary skill in the art at the time the invention was made to update the subscriber keys corresponding to at least one subscriber when the at least one subscriber's set of subscriber keys comprises an amount of active keys that falls below 1, as taught by Wallner. One would have been motivated to do so because when the number of keys falls below 1, there are no more active keys by which legal subscribers can decrypt data, which is counterproductive. This coupled with the fact that Wallner teaches only 1 active key, means that it is necessarily the case that after the number of keys falls below 1, an update would be necessary.

6.2 Claims 5, 14-17, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Efficient Methods for Integrating Traceability and Broadcast Encryption" to Gafni et al. (Gafni) in view of "Key Management for Multicast: Issues and Architecture" to Wallner et al. (Wallner) as applied to claims 4, 12, and 19 above respectively and further in view of "Coding for Blacklisting Problems Without Computational Assumptions" to Kumar et al. (Kumar).

As per claims 5, 14, and 20, the Gafni-Wallner combination teaches the limitations of the base claims, but fails to explicitly teach "tracking a total amount of compromised cards; and encoding a smartcard with the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold." However, Kumar in an analogous art teaches "tracking a total amount of compromised cards; and encoding a smartcard with the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold." Specifically, as per encoding a smartcard with the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold, see Kumar, page 619, "The Outer Code", in which updating need only be done after a predetermined communication blowup threshold.

As per tracking a total amount of compromised cards, examiner respectfully asserts that it is necessarily the case that Kumar's teaching suggests tracking the number of compromised cards, because this would be necessary in order to determine when updating is needed which he does explicitly teach as pointed out above.

As per claim 17 the Kumar further teaches "wherein K, r, and d are selected to obtain a bound on the number of subscribers that are reissued smartcards in recarding sessions." See page 617 "The Inner code."

It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the Gafni-Wallner combination such that the process of updating included "tracking a total amount of compromised cards; and encoding a smartcard with the updated set of subscriber keys when the total amount of compromised cards meets a second predefined threshold," and "wherein K, r, and d are selected to obtain a bound on the number of subscribers that are reissued smartcards in recarding sessions." One would have been motivated to do so because this would allow for more efficient updates, taking place only when needed.

As per claim 15, the Gafni-Wallner-Kumar combination teaches all limitations of base-claim 14. Kumar further teaches wherein d is substantially equal to K/r, as admitted by the applicant on page 15, lines 9-13 of the disclosure.

As per claim 16, the Gafni-Wallner-Kumar combination teaches all limitations of base-claim 14. Wallner further teaches "wherein the step of reissuing comprises the steps of: generating a new key for each compromised key to update the universal set of keys; and randomly selecting r keys from the updated universal set of keys to generate the updated set of subscriber keys" see pages 7-8, "5.4.1 The Exclusion Principle". It would have been obvious to one having ordinary skill in the art at the time the invention was made to include the steps taught by Wallner of reissuing comprising generating a new key for each compromised key to update the universal set of keys; and randomly selecting r keys from the updated universal set of keys to generate the updated set of subscriber keys. One would have been motivated to do so because the scheme includes many benefits, such as "the costs of user storage and rekey transmissions are balanced and scalable as the number of users increases." See page 8, the section labeled "The Benefits of a scheme such as this are:"

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following is a list of pertinent prior art US Patents:

US005325432A

US006567914B1

US005361256A

US006131160A

US 20020129249A1

US006055314A

US006094487A

US005592552A

US006463155B1

US 20030169885A1

The following is a list of pertinent nonpatent documents:

Wallner et al. Key Management for Multicast:Issues and Architectures. Internet Draft, June 1999.

Kumar et al. "Coding Constructions for Blacklisting Problems without Computational Assumptions," in Advances in Cryptology -- Crypto '99, LNCS 1666, pages 609--623, 1999.

Gafni et al. "Efficient Methos for Integrating Traceability and Broadcast Encryption" UCLA. -- Crypto '99, LNCS 1666, pages 372-387, 1999.

Decatur et al. "A Probabilistic Error-Correcting Scheme" Internet Draft. June 25, 1997.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali M. Mashaal whose telephone number is 703-305-7854. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

AM

Emmanuel L Moise
EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136